

06-60310

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
CR - MIDDLEBROOKS

Case No. _____
18 USC 1030(a)(5)(A)(i)

MAGISTRATE
JOHNSON

UNITED STATES OF AMERICA

v.

JOSEPH HARLEN SHOOK,

Defendant.

FILED BY: _____ J.C.
2006 NOV -2 PM 3:00
CLERK
S.D. OF FLORIDA

INDICTMENT

The Grand Jury charges that:

GENERAL ALLEGATIONS

At times material to this Indictment:

A. Muvico Entertainment, LLC

1. Muvico Entertainment, LLC ("Muvico"), was incorporated in Florida, and has its headquarters located at 3101 N. Federal Highway, Fort Lauderdale, Florida 33306. Muvico was in the business of running multiplex movie theaters in and outside of the state of Florida.

2. Muvico used computers in interstate commerce and communication. Among other such uses, Muvico maintained a website at "www.muvico.com" that could be accessed by computers connected to the Internet. The Muvico website allowed Muvico patrons to purchase their tickets in

advance over the Internet to movies showing at Muvico theater facilities. Muvico also used the Internet to link the ticket sales computers at each of the company's twelve theaters, with computers located at the company headquarters in Fort Lauderdale, Florida. The theater locations and headquarters were linked together in such a network so that individual theaters could electronically communicate with each other and with Muvico headquarters. Although the Internet was used to create this networking link, various electronic security measures, such as an encrypted Virtual Private Network ("VPN"), were taken in order to secure communications between the theater locations and headquarters.

3. Muvico employed two wireless networking devices at the company headquarters facility in Fort Lauderdale. These wireless devices were components of smaller sub-networks within Muvico's primary network, which included most of the computers at Muvico's headquarters facility, as well as computers at the twelve theater locations. The wireless components were protected by a 26-character encryption password. Once a computer was connected to the Muvico network via one of these wireless gateways, this computer had direct access to computers at headquarters and computers at the twelve theater locations. The computers at each theater location contained the hardware and software necessary to manage on-site and online movie ticket sales, as well as to process all credit card transactions.

4. The wireless networking devices employed by Muvico transmitted their beacons approximately 100 yards. Consequently, despite Muvico's security measures, a person with knowledge of Muvico's computer and security systems could access Muvico's computer system from outside Muvico's headquarters building.

B. The Attack on the Muvico Computer System

5. On or about May 5, 2006, Mission Impossible III was scheduled to premiere at numerous movie theaters, including Muvico movie theaters. Mission Impossible III was expected to be one of the highest-grossing films of the late spring/early summer movie season.

6. Also on or about May 5, 2006, coinciding with the premiere of Mission Impossible III, six of Muvico's highest grossing theaters (Muvico Palace 20 in Boca Raton, Florida; Muvico Egyptian 24 in Hanover, Maryland; Muvico Paradise 24 in Davie, Florida; Muvico Baywalk 20 in St. Petersburg, Florida; Muvico Starlight 20 in Tampa, Florida; and Muvico Parisian 20 in West Palm Beach, Florida) experienced disruptions to their on-site and www.muvico.com website ticket sales systems, and also experienced disruption in the processing of credit card transactions at theater locations. As a result, the affected Muvico theaters could sell tickets for cash only and suffered an estimated sales loss of approximately \$100,000.00.

7. Muvico maintained digital log files of activities on their network. These log files showed that the intruder into the Muvico computer system who caused the May 5, 2006 attack, made entry through a wireless networking device at Muvico headquarters, and used a wireless networking adapter bearing Media Access Control ("MAC") address 00:16:01:18:0C:1A. A MAC address is a unique twelve-digit code assigned to most forms of computer-networking hardware, which is "burned," or permanently written into the hardware by the manufacturer.

C. Joseph Harlen Shook

8. Defendant **JOSEPH HARLEN SHOOK** was employed by Muvico from on or about May 19, 2003, through on or about February 17, 2006, when Muvico terminated his employment.

9. For approximately the last year of defendant **JOSEPH HARLEN SHOOK**'s employment

with Muvico, defendant **JOSEPH HARLEN SHOOK** served as the Director of Information Technology. As such, he was responsible for the computer security policy in place at the time of the May 5, 2006, attack on the Muvico computer system.

10. Upon defendant **JOSEPH HARLEN SHOOK**'s termination from Muvico, he was no longer permitted to access the Muvico network, other than as any other lawful patron of Muvico could, by accessing the Muvico web site located at www.muvico.com.

11. On or about September 6, 2006, defendant **JOSEPH HARLEN SHOOK** was found in possession of the wireless networking adapter bearing MAC address 00:16:01:18:0C:1A.

COUNT 1

12. The allegations contained in the General Allegations Section of this Indictment are incorporated herein as though fully realleged.

13. On or about May 5, 2006, in Broward County, in the Southern District of Florida, and elsewhere, the defendant,

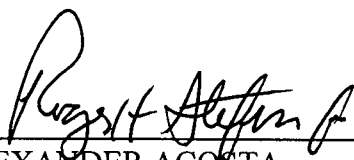
JOSEPH HARLEN SHOOK,

knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, to wit,

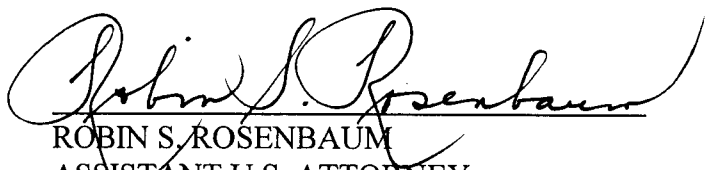
the computer system of Muvico, in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i) and 2.

A TRUE BILL

GRAND JURY FOREPERSON



R. ALEXANDER ACOSTA
UNITED STATES ATTORNEY



ROBIN S. ROSENBAUM
ASSISTANT U.S. ATTORNEY